CLAIMS

1. A method for encoding a m-bit chain wherein the errors do not spread on more than n bits, n being lesser or equal to m, said method comprising the steps of:

- choosing an irreducible generator polynomial of degree p, p being greater or equal to n and such that m is lesser or equal to $p(2^p-1)$;

- building a matrix (400) using 2^p elements of the galois field (200) GF, generated by the generator polynomial, comprising the 2^p-1 elements of the multiplicative group a^0, a^1, a^2 ...a^{p-1} and $\varnothing$ (210), the null element for the addition and, using p x p blocks wherein the first line is one first element and the other lines are the other elements of the GF multiplicative group obtained by a circular permutation of the first line, in the following way:

  - defining a first set of p columns (521) comprising a succession of 2^p+2 blocks wherein the first lines are respectively $\varnothing$,$\varnothing$ and 2p times a^0;

  - defining a second set of p columns (522) comprising a succession of 2^p+2 blocks wherein the first lines are successively $\varnothing, a^0, \varnothing, a^0$, a^1, a^2 ...a^{p-1};

  - defining a third set of p columns (523) comprising a succession of 2^p+2 blocks wherein the first lines are successively $a^0, \varnothing, \varnothing, a^0, a^0, (a^{p-1})^{-1}$, $(a^{p-2})^{-1}$... $(a^1)^{-1}$.

- computing a bit chain code for the m-bit chain by performing a matrix multiplication of a bit chain wherein the m MSB bits are the m-bit chain and the remaining LSB bits are all-zero, by the previously built matrix and appending to the m-bit chain the bit chain code as new LSB bits.

2. The method of claim 1 wherein the choosing step consists in choosing the generator polynomial

$G(X) = X^8 + X^4 + X^3 + X^2 + 1$

m being assigned to 512, p being assigned to 8.

3. The method of claim 2 further comprising as the last step for building a matrix, the step of:
suppressing from the just built matrix (900), the first three columns, the three last rows of the third 8x8 blocks for each column, the five last rows of the fourth 8x8 blocks for each column, the three last rows of the 2060 following 8x8 blocks for each column and the five last rows of the last block for each column.

4. The method of claim 1 wherein the building step further comprises the following steps of:
- suppressing the third set of p columns (523);
- suppressing the first p rows in the first (421) and second (422) sets of p columns.

5. A method for decoding a received bit chain wherein the errors do not spread on more than n bits, said received bit chain comprising a m bit chain formed by the m MSB bits and a code bit chain formed by the p remaining LSB bits, p being the degree of an irreducible generator polynomial, p being greater or equal to n and such that m is lesser or equal to $p(2^p-1)$, said method comprising the steps of:
- building a matrix (400) using 2^p elements of the galois field GF, generated by the generator polynomial comprising the 2^p-1 elements of the multiplicative group (200), a^0, a^1, a^2 ...a^{p-1} and Ø (210), the null element for the addition and, using p x p blocks wherein the first line is one first element and the other

lines are the other elements of the GF multiplicative group obtained by a circular permutation of the first line, in the following way:

- defining a first set of p columns (521) comprising a succession of 2^p+2 blocks wherein the first lines are respectively $\varnothing, \varnothing$ and 2p times a^0;
- defining a second set of p columns (522) comprising a succession of 2^p+2 blocks wherein the first lines are successively $\varnothing, a^0, \varnothing, a^0, a^1, a^2 \ldots a^{p-1}$;
- defining a third set of p columns (523) comprising a succession of 2^p+2 blocks wherein the first lines are successively $a^0, \varnothing, \varnothing, a^0, a^0, (a^{p-1})^{-1}, (a^{p-2})^{-1} .. (a^1)^{-1}$.

- computing a syndrome bit chain for the received bit chain by performing a matrix multiplication of said received bit chain by the previously built matrix;
- correcting errors introduced in one of the 2^p-1 x p bit sub chains forming the m MSB bits of the received bit chain by executing the following steps:
  - performing a division (800, 810, 830) in the GF, the divider being Sa, a p-bit chain formed by the p MSB bits of the syndrome bit chain, the dividend being Sb, the following p MSB bits after Sa of the syndrome bit chain and obtaining an exact quotient p bit chain;
  - using the exact quotient as a range of the p bit sub chain in the m MSB bits of the received bit chain to select (870) a p bit sub chain containing errors; and,
  - taking Sa (880) as an error pattern, changing (890) the value of each bit of the selected p bit sub chain at the location identified by the bits in Sa which are set to 1.

6. The method of claim 5 wherein the steps for correcting errors further comprise the following step for correcting errors in the bit chain code:

- correcting (860) a p-bit sub chain (850) of the bit chain code by applying as an error pattern, the p-bit chain (855) formed by a p-bit sub chain in the syndrome bit chain having the same range in the syndrome than the P-bit sub chain in the bit chain code.

7. The method of claim 5 further comprising, before the steps for correcting errors, the following steps for detecting the errors in the $2^{p}-1$ x p bit sub chains forming the m MSB bits of the received bit chain:

- if the p bit syndrome is all-zero (750), concluding that there is no error (770) and skipping the execution of the steps for correcting errors;
- detecting if the errors are correctable by executing the following steps:
    - computing in the GF (705, 710, 720, 730), the two elements of the GF Sa^2 and Sb x Sc, Sc being the p LSB bits of the syndrome bit chain;
    - comparing (740) the two elements Sa^2 and Sb x Sc;
    - if the compared elements are different, concluding that the errors are uncorrectable (745) and skipping the execution of the correcting steps;
    - if the compared elements are identical and if Sa is not all-zero, concluding (760) that the errors are correctable and executing the steps for correcting errors.

8. The method of claim 7 further comprising for detecting errors in the bit chain code of the receiving bit chain the steps of:

- determining (750) if a p-bit sub chain of the bit chain code is not all-zero and if said p-bit chain is not all-zero (765), applying the step for correcting errors in the bit chain code to said p-bit sub chain of the bit chain code.

9. The method of claim 8 wherein the step of computing a division in the GF comprises the following steps:
- creating a lookup table (800, 810), associating an index from 0 to 2^{p-1} to each element of the GF multiplicative group, said index being the rank of the GF element in the GF multiplicative group;
- associating an index Ib to Sb and an index Ia to Sa by reading the lookup table;
- performing a substraction (830) modulo 2^{p-1} of Ib+2^{p-1} minus Ia;
- reading in the lookup table the GF element corresponding to the resulting index of the substraction the resulting index obtained in the performing a substraction step, the GF element being the result of the step of computing a division in the GF.

10. The method of claim 8 wherein the step of computing in the GF, the two elements Sa^2 and Sb x Sc comprises the following steps:
- creating a lookup table (700, 710, 720), associating an index from 0 to 2^{p-1} to each element of the GF multiplicative group, said index being the rank of the GF element in the GF multiplicative group;
- associating an index Ib to Sb, an index Ic to Sc and an index Ia to Sa by reading the lookup table;
- performing an addition (730) modulo 2^{p-1} of Ia and Ia;
- performing an addition (735) modulo 2^{p-1} of Ib and Ic;
- reading in the lookup table the two GF elements corresponding to the two resulting index of the two additions, the two GF elements being the two results of the step of computing in the GF, the two elements Sa^2 and Sb x Sc.

11. The method of claim 8 wherein the step of computing in the GF, the two elements Sa^2 and Sb x Sc comprises the following steps:

- creating a first lookup table having 2^{p-1} entries, associating to each element of the GF, its square value computed modulo 2^{p-1};
- creating a second lookup table having 2^{p-1} X 2^{p-1} entries, each entry being the GF element corresponding to one possible precomputed product of two GF elements;
- reading respectively in the lookup tables the two GF elements corresponding to Sa^2 and to the product Sb x Sc.

12. The method of claim 11 wherein the choosing step consists in choosing the generator polynomial

$G(X) = X^8 + X^4 + X^3 + X^2 + 1$

m being assigned to 512, p being assigned to 8.

13. The method of claim 12 further comprising as the last step for building a matrix, the step of:

suppressing from the just built (2064,24) matrix (900), the first three columns, the three last rows of the third 8x8 blocks for each column, the five last rows of the fourth 8x8 blocks for each column, the three last rows of the 2060 following 8x8 blocks for each column and the five last rows of the last block for each column.

14. The method of claim 6 wherein the building step further comprises the following steps of:

- suppressing the third set of p columns (523);
- suppressing the first p rows in the first (421) and second (422) set of p columns.

15. An apparatus for encoding a m-bit chain wherein the errors do not spread on more than n bits, n being lesser or equal to m, said apparatus comprising means adapted for carrying out the method according to anyone of claims 1 to 4.

16. An apparatus for decoding a m-bit chain wherein the errors do not spread on more than n bits, n being lesser or equal to m, said apparatus comprising means adapted for carrying out the method according to anyone of claims 5 to 14.